Kentucky.gov

Commonwealth Office of Technology

From: Ritchey, Gail (COT)
Sent: Wednesday, January 16, 2008 10:40 AM
To: COT Constitutional CIO Security Contacts; COT Cabinet CIO Security Contacts; CTC Members
Cc: COT Exchange Administrators; COT Security Alert Contacts; COT Security Contact COT-Support; COT Security Contact Pass; COT Security Contact Self-Support; COT Technical Contacts; SecurityContacts Group
Subject: Current Malicious Code Vulnerabilities

COT Security Alert

The Commonwealth Office Technology has been made aware of several malicious codes that may pose a threat to systems within state government.

- W32.Forbot.A
- W32.Fishinflu @ mm *(name edited slightly for security)*
- W32.Ackpra.A
- W32.Sdbot.DJU

These are worms or trojans that have some or all of these capabilities: destroying data, bypassing security software, stealth, stealing information, remote exploitation and downloading other code.

Strategies to use against these threats include:

- Never open or execute files from unknown sources or unexpected email attachments from known sources.
- Turn off file-sharing if not needed.
- Ensure security patches are installed as available.
- Ensure all antivirus definitions are up-to-date.

These strategies work best if practiced at all times.

NOTICE: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for

these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

Commonwealth Office of Technology
Division of Technical Services
Security Administration Branch
120 Glenn's Creek Road, Jones Building
Frankfort, KY 40601
COTSecurityServices@ky.gov
http://technology.ky.gov/security/